UNITED STATES PATENT AND TRADEMARK OFFICE

9

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/390,363 | 09/07/1999 | JON N. LEONARD | BEU/LEONARD | 6725 |

7590 05/18/2005

BACON & THOMAS
625 SLATERS LANE 4TH FLOOR
ALEXANDRIA, VA 223141176

| EXAMINER | |
|---|---|
| DADA, BEEMNET W | |
| ART UNIT | PAPER NUMBER |
| 2135 | |

DATE MAILED: 05/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

|  |  |  |
|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>09/390,363 | **Applicant(s)**<br>LEONARD ET AL. |
|  | **Examiner**<br>Beemnet W. Dada | **Art Unit**<br>2135 |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *06 January 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

## DETAILED ACTION

1. This office action is in reply to an amendment filed on January 06, 2005. Claims 1 and 41 have been amended. Claims 1-50 are pending.

### *Claim Rejections - 35 USC § 103*

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anderson (US Patent No. 6,442,600 B1) in view of Ogilvie et al. (hereinafter Ogilvie) (US Patent No. 6,324,569 B1).

4. As per claim 1, Anderson discloses an electronic mail system (i.e. system for distributing electronic messages, see figure 1) comprising:

a first computer 150 (i.e. the sender, see column 3 lines 61-63) which is connect to a network 140 capable of carrying an electronic mail message (i.e. transmission of the electronic messages, see column 4 line 65- column 5 line 1);

recipient computers systems (elements 160, 170, and 180; see figure 1) are connected to network 140 [see column 4 lines 59-65];

a view applet (i.e. the message receiver 155 with the URL, the web browser software, see column 4 lines 13-16);

Anderson discloses the electronic message (i.e. e-mail) includes minimum or maximum expiration time periods (i.e. time is attached to the electronic mail message prior to transmission over network, see column 3 lines 62-67) will cause the electronic message and all designated incarnations thereof to expire. Anderson also discloses the electronic message (i.e. e-mail) is encrypted so that it may only be viewed using said view applet (i.e. URL web browser) upon installation of said view applet on the recipient computers (i.e. element 160, 170, 180, see figure I and column 5 lines 25-30).

Furthermore, Anderson teaches deleting encrypted message when time period that is associated with the message has expired [column 4, lines 30-35, column 5, lines 24-26]. Anderson also teaches providing recipient access restrictions [column 4, lines 3-7]. Anderson does not explicitly teach a viewer applet arranged to prevent decryption and viewing of encrypted messages by a recipient after the occurrence of date, time or event selected by the originator of the message.

Ogilvie teaches an electronic mail system (see figure 1 and column 3, lines 47-57), including attaching processing limitations during creation of electronic mail at the originator / intermediate node (for example, attaching a removal code for deleting electronic mail after a certain period of time (see columns 5, 6 lines 45-55, sections a-l), encrypting electronic mail (see column 5, lines 10-15)). Oglivie further teaches decrypting at the recipient mailbox encrypted electronic messages and displaying the message (i.e., the viewer applet is arranged to decrypt the electronic mail message to permit viewing of said electronic message, Note that if the expiration date/time occurs the electronic message is erased which implies the message is decrypted before the occurrence of the expiration date/time (see column 16, lines 7-20)), deleting messages (encrypted / non-encrypted messages) from each recipient mailbox according to the processing limitations set by the originator software (i.e., removing messages after a certain period of time at the recipient viewer applet thereby preventing viewing and decrypting of messages, since messages are deleted from the mail box (see column 5, lines 60-65, column 6, sections a-l, column 7, lines 27-39, column 16, lines 7-21).

Both Anderson and Ogilive teach a method of controlling electronic messages. It would have been obvious to one having ordinary skill in the art at the time the invention was made to prevent decryption and viewing of encrypted messages by a recipient after the occurrence of date, time or event selected by the originator of the message at the recipient as taught by Ogilvie and incorporate it within the electronic mail system of Anderson, in order to further delete stored messages at the user applet according to attached limitations and further provide an improved approach to method of removing of email messages as suggested by Ogilvie [column 2, lines 14-24].

5. As per claim 18, Anderson teaches a method of controlling an electronic mail message transmitted over a network, comprising the steps of:

before transmission of the electronic mail message over the network, attaching to the message a date, time, or event, the occurrence of which will cause said electronic mail message and all designated incarnations thereof to expire (column 3, lines 62-67); and

encrypting said electronic mail message so that it can only be viewed before the occurrence of said time, date or event using viewer applet installed on recipient computer (column 5, lines 25-30, and column 4, lines30-34). Furthermore, Anderson teaches deleting encrypted message when time period that is associated with the message has expired [column 4, lines 30-35, column 5, lines 24-26]. Anderson also teaches providing recipient access restrictions [column 4, lines 3-7]. Anderson does not explicitly teach a viewer applet arranged to prevent decryption and viewing of encrypted messages by a recipient after the occurrence of date, time or event selected by the originator of the message.

Ogilvie teaches an electronic mail system (see figure 1 and column 3, lines 47-57), including attaching processing limitations during creation of electronic mail at the originator / intermediate node (for example, attaching a removal code for deleting electronic mail after a certain period of time (see columns 5, 6 lines 45-55, sections a-l), (see columns 5, 6 lines 45-55, sections a-l), encrypting electronic mail (see column 5, lines 10-15)). Ogilvie further teaches deleting messages (encrypted / non-encrypted messages) from each recipient mailbox according to the processing limitations set by the originator software (i.e., removing messages after a certain period of time at the recipient viewer applet thereby preventing viewing and decrypting of messages, since messages are removed from the mail box (see column 5, lines 60-65, column 6, sections a-l, column 7, lines 27-39, column 16, lines 7-21).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to prevent decryption and viewing of encrypted messages by a recipient after the occurrence of date, time or event selected by the originator of the message at the recipient as taught by Ogilvie and incorporate it within the electronic mail system of Anderson, in order to further delete stored messages at the user applet according to attached limitations and further provide an improved approach to method of removing of email messages as suggested by Ogilvie [column 2, lines 14-24].

6. As per claim 34, Anderson discloses an electronic mail system (i.e. system for distributing electronic messages, see figure 1) comprising

a) a first computer 150 (i.e. the sender, see column 3 lines 61-63) on which is installed message origination software (i.e. message sender software 154, see figure 1) and which is connect to a network 140 capable of carrying an electronic mail message (i.e. transmission of the electronic messages, see column 4 line 65- column 5 line l), said message origination software being arranged to enable an originator of the message to attach message processing limitations to the message before it is sent (i.e. minimum or maximum expiration time is attached to the electronic mail message prior to transmission over network, see column 3 lines 62-67);

b) recipient computers systems (elements 160, 170, and 180; see figure 1) are connected to network 140 [see column 4 lines 59-65],

c) a viewer applet (i.e. the message receiver 155 with the URL, the web browser software, see column 4 lines 13-16);

d) a central electronic mail server (i.e. Message Distribution server (MDS), see figure 1) connected to the network 140. Anderson discloses the message sender to supply the electronic message to the MDS and the MDS will stores the message and is responsible for forwarding it to the recipient [see column 5 lines 19-50]. Anderson also discloses the MDS will retrieve the public key from the recipient and encrypt the electronic message upon request by the recipient and stream it to corresponding recipient [see figure 6 steps 625,630,635,40]. The recipient can access the message by decrypting it using the private key of the recipient computer system's private key and display said electronic message [see column 6 lines 16-29].

Anderson also discloses the processing limitations (i.e. restriction on access by some or all recipients, see column 3 line 65-column 4 line 1) are implemented by said central electronic mail server (i.e. MDS) and message receiver 155 (i.e. said view applet, see figure 1). Anderson does not explicitly teach a viewer applet arranged to prevent decryption and viewing of encrypted messages by a recipient after the occurrence of date, time or event selected by the originator of the message.

Ogilvie teaches an electronic mail system (see figure 1 and column 3, lines 47-57), including attaching processing limitations during creation of electronic mail at the originator / intermediate node (for example, attaching a removal code for deleting electronic mail after a certain period of time (see columns 5, 6 lines 45-55, sections a-l), (see columns 5, 6 lines 45-55, sections a-l), encrypting electronic mail (see column 5, lines 10-15)). Ogilvie further teaches deleting messages (encrypted / non-encrypted messages) from each recipient mailbox according to the processing limitations set by the originator software (i.e., removing messages after a certain period of time at the recipient viewer applet thereby preventing viewing and decrypting of messages, since messages are removed from the mail box (see column 5, lines 60-65, column 6, sections a-l, column 7, lines 27-39, column 16, lines 7-21).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to prevent decryption and viewing of encrypted messages by a recipient after the occurrence of date, time or event selected by the originator of the message at the recipient as taught by Ogilvie and incorporate it within the electronic mail system of Anderson, in order to further delete stored messages at the user applet based on attached limitations and further provide an improved approach to method of removing of email messages as suggested by Ogilvie [column 2, lines 14-24].

7. As per claim 41, Anderson discloses a computer program for handling electronic mail comprising: a) a mail original portion (i.e. message sender 154, see figure 1) arranged to permit the sender to supply messaging sending information including optional information as minimum and maximum expiration time (i.e. a date, time or event, see column 3 lines 62-65). The Message Receiver (MR) stores the decrypted message indicator (i.e. e-mail) in an encrypted fashion on the recipient computer system [see column 6 lines 16-29] and erase (i.e. delete) the

message if the expiration period has ended (i.e., upon the occurrence of said date, time, or event, see column 9 lies 64-66). b) a view applet portion (i.e. message receiver 155, see figure 1) arranged to access the message by decrypting it using the private key of the recipient computer system's private key and display said electronic message [see column 6 lines 16-29] and. permit viewing of the received electronic message before the expiration time period end [see column 9 lines 66-67]. Anderson does not explicitly teach a viewer applet arranged to prevent decryption and viewing of encrypted messages by a recipient after the occurrence of date, time or event selected by the originator of the message.

Ogilvie teaches an electronic mail system (see figure 1 and column 3, lines 47-57), including attaching processing limitations during creation of electronic mail at the originator / intermediate node (for example, attaching a removal code for removing an electronic mail after certain time period (see columns 5, 6 lines 45-55, sections a-l), encrypting electronic mail (see column 5, lines 10-15)). Oglivie further teaches decrypting at the recipient mailbox encrypted electronic messages and displaying the message (i.e., the viewer applet is arranged to decrypt the electronic mail message to permit viewing of said electronic message, (see column 16, lines 7-20)), deleting messages (encrypted / non-encrypted messages) from each recipient mailbox according to the processing limitations set by the originator software (i.e., removing messages after a certain period of time at the recipient viewer applet thereby preventing viewing and decrypting of messages, since messages are removed from the mail box (see column 5, lines 60-65, column 6, sections a-l, column 7, lines 27-39, column 16, lines 7-21).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to prevent decryption and viewing of encrypted messages by a recipient after the occurrence of date, time or event selected by the originator of the message at the recipient as taught by Ogilvie and incorporate it within the electronic mail system of Anderson, in order to further delete stored messages at the user applet based on attached limitations and further provide an improved approach to method of removing of email messages as suggested by Ogilvie [column 2, lines 14-24].

8. As per claims 2-3, 8-9, 19-20, 24-25, 35 and 42 the combination of Anderson and Ogilvie teaches the system as applied above. Furthermore, Anderson teaches the electronic mail system (i.e. system for distributing electronic messages, see figure 1) further comprising a central electronic mail server (i.e. Message Distribution server (MDS), see figure 1) connected to the network 140. Anderson discloses the message sender to supply the electronic message to the MDS and the MDS will stores the message and is responsible for forwarding it to the recipient [see column 5 lines 1950]. Anderson also discloses the MDS will retrieve the public key from the recipient and encrypt the electronic message upon request by the recipient and stream it to corresponding recipient [see figure 6 steps 625,630,635,640]. The recipient can access the message by decrypting it using the private key of the recipient computer system's private key and display said electronic message [see column 6 lines 16-29].

9. As per claims 4-5, 21 and 36-37, the combination of Anderson and Ogilvie teaches the system as applied above. Furthermore, Anderson discloses the recipient (i.e. a user) can select a message and indicate a message forwarding action to be taken (i.e. forward to a second recipient computer, see figure 2 and column 6 lines 46-65). Anderson discloses the message distributor subroutine of MDS (i.e. central mail server) being arrange to encrypt the message using the public encryption key generated in the recipient computer s, stem [see column 5 lines 58-63] and send it to each Y recipient [column 9 lines 9-16].

10. As per claims 6-7 and 22-23, the combination of Anderson and Ogilvie teaches the system as applied above. Furthermore, Anderson discloses the central electronic mail server (i.e. MDS) erases (i.e. deletes) the single copy of the electronic message when the end of a maximum time period has expired [see column 4 lines 25-44].

11. As per claims 10-12 and 26-28, the combination of Anderson and Ogilvie teaches the system as applied above. Furthermore, Anderson discloses the electronic message (i.e. E-mail) is encrypted in the central mail server (i.e. Message Distribution Server) with the recipient's public key before transmission to said recipient computer [see column 10 lines 5-14 and figure 6 steps 625,630,635,640].

12. As per claims 13, 29 and 43, the combination of Anderson and Ogilvie teaches the system as applied above. Furthermore, Ogilvie teaches deleting messages (encrypted / non-encrypted messages) from each recipient mailbox according to the processing limitations set by the originator software (i.e., removing messages after a certain period of time at the recipient viewer applet thereby preventing viewing and decrypting of messages, since messages are removed from the mail box (see column 5, lines 60-65, column 6, sections a-l, column 7, lines 27-39, column 16, lines 7-21).

13. As per claims 14-15 and 30-31, the combination of Anderson and Ogilvie teaches the system as applied above. Furthermore, Anderson discloses the recipient (i.e. a user) can select a message and indicate a message forwarding action to be taken (i.e. forward to a second recipient computer, see figure 2 and column 6 lines 46-65). Anderson discloses the message distributor subroutine of MDS (i.e. central mail server) being arrange to encrypt the message

using the public encryption key generated in the recipient computer system [see column 5 lines 58-63] and send it to each recipient [column 9 lines 9-16].

14. As per claims 16, 32 and 44, the combination of Anderson and Ogilvie teaches the system as applied above. Furthermore, Anderson discloses the message origination software (i.e. message sender 154, see figure 1) arranged to permit the message to include the expiration time (i.e. limitation, see column 3 lines 62-65) before transmission over said network 140 [see column 3 lines 48-66 and figure 2).

15. As per claims 17, 33 and 45, the combination of Anderson and Ogilvie teaches the system as applied above. Furthermore, Ogilvie teaches deleting messages (encrypted / non-encrypted messages) from each recipient mailbox according to the processing limitations set by the originator software (i.e., removing messages after a certain period of time at the recipient viewer applet thereby preventing viewing and decrypting of messages, since messages are removed from the mail box (see column 5, lines 60-65, column 6, sections a-l, column 7, lines 27-39, column 16, lines 7-21).

16. As per claims 38-40, the claimed steps correspond to the functions of the elements of the apparatus claims 34-37, which has been rejected above and thus rejected with the same reason applied thereto.

17. As per claims 46-50, the claimed steps Correspond to the functions of the elements of the apparatus claims 41-45, which has been rejected above, and thus rejected with the same reason applied thereto.

### ***Response to Arguments***

18. Applicant's arguments filed January 06, 2005 have been fully considered but they are not persuasive. Applicant argues that neither Anderson nor Oglivie disclose or suggest use of viewer applet that is arranged to decrypt electronic mail message to permit viewing of the electronic message before the occurrence of the date, time or event selected by the originator of the electronic message and to prevent decryption and viewing of the electronic message by the recipient after the occurrence of the date, time or event selected by the originator of the message. Examiner respectfully disagrees.

It is understood by the examiner in view of the specification that electronic messages are prevented from decryption and viewing at the recipient when the message itself and/or decryption key is **erased form the recipient** system after occurrence of expiration time or date, wherein the expiration time or date is set at the originator of the message. Examiner would point out that Ogilive teaches an electronic mail system (see figure 1 and column 3, lines 47-57), including attaching processing limitations during creation of electronic mail at the originator / intermediate node (for example, attaching a **removal code for deleting electronic mail after a certain period of time** (see columns 5, 6 lines 45-55, sections a-l), encrypting electronic mail (see column 5, lines 10-15)). Oglivie further teaches decrypting at the recipient mailbox, encrypted electronic messages and displaying the message (i.e., the viewer applet is arranged to decrypt the electronic mail message to permit viewing of said electronic message, Note that if the expiration date/time occurs the electronic message is erased which implies the system is arranged to decrypt and view the message before the occurrence of the expiration date/time otherwise the message won't be available to be decrypted and viewed (see column 16, lines 7-20 and column 5,6 sections a-l)) deleting messages (encrypted / non-encrypted messages) from each recipient mailbox according to the processing limitations set by the originator software (i.e., **removing messages after a certain period of time at the recipient viewer applet thereby preventing viewing and decrypting of messages, since messages are deleted from the mail box** (see column 5, lines 60-65, column 6, sections a-l, column 7, lines 27-39, column 16, lines 7-21).

19. Applicant further argues that the reason that Ogilvie includes expiration data is so that the recipient does not have to bother with deletion of the e-mail, and Ogilvie does not teach the type of encryption that enables originator or sender control of message. Examiner disagrees.

Examiner would point out that, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. In a claim drawn to a process of making, the intended use must result in a manipulative difference as compared to the prior art. See *In re Casey*, 370 F.2d 576, 152 USPQ 235 (CCPA 1967) and *In re Otto*, 312 F.2d 937, 939, 136 USPQ 458, 459 (CCPA 1963). In this case both the present claimed invention and Ogilive use erasing of electronic message after expiration time/date. The intended use of Ogilvie may be different from the present invention, however erasing of the electronic message wherein the originator sets the expiration time meets the claimed limitation.

20. Applicant further argues that neither Anderson nor Ogilvie suggest the use of a central server to stream messages to an expiration-date controlling viewer applet on the recipient's computer. Examiner disagrees.

Examiner would point out that Anderson discloses the recipient (i.e. a user) can select a message and indicate a message forwarding action to be taken (i.e. forward to a second recipient computer, see figure 2 and column 6 lines 46-65). Anderson discloses the message distributor subroutine of MDS (i.e. central mail server) being arrange to encrypt the message using the public encryption key generated in the recipient computer s, stem [see column 5 lines 58-63] and send it to each Y recipient [column 9 lines 9-16].

## *Conclusion*

21. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

May 10, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100